UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 09/898,184 | 07/03/2001 | Nicol Chung Pang So | 018926-006610US | 9607 |

20350 7590 04/07/2006

TOWNSEND AND TOWNSEND AND CREW, LLP
TWO EMBARCADERO CENTER
EIGHTH FLOOR
SAN FRANCISCO, CA 94111-3834

| EXAMINER | |
|---|---|
| DADA, BEEMNET W | |
| ART UNIT | PAPER NUMBER |
| 2135 | |

DATE MAILED: 04/07/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

| Office Action Summary | Application No.<br>09/898,184 | Applicant(s)<br>SO ET AL. | |
|---|---|---|---|
| | Examiner<br>Beemnet W. Dada | Art Unit<br>2135 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *04 January 2006*.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-9,11-19,33,34 and 40-42* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-9, 11-19, 33, 34 and 41-42* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) □ Notice of References Cited (PTO-892)
2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) □ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .
5) □ Notice of Informal Patent Application (PTO-152)
6) □ Other: _____.

## DETAILED ACTION

1. This office action is in reply to an amendment file don January 04, 2006. Claims 1, and 41 to have been amended, claims 20-32 and 35-37 have been cancelled. Claims 1-9, 11-19, 33, 34 and 40-42 are pending.

### *Claim Objections*

2. Claim 40 is objected to because of the following informalities: Claims 40 depends on cancelled claim 20. Appropriate correction is required.

### *Claim Rejections - 35 USC § 112*

3. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

4. Claims 1, 2, 41 and 42 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. The specification fails to mention or teach encryption renewal system performs periodic entitlement control message renewal in synchronization with a conditional access system **and without re-encrypting the pre-encrypted content**.

### *Claim Rejections - 35 USC § 103*

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 1-2 and 41-42 are rejected under 35 U.S.C. 103(a) as being unpatentable over Colligan et al US Patent 6,415,031 B1 (hereinafter Colligna) in view Wasilewski et al. US Patent 6,516,412 B2 (hereinafter Wasilewski).

7. As per claims 1 and 41, Colligan discloses a system for delivering content to a subscriber terminal on-demand through a communication network (see for example; abstract and fig 4), the system comprising:

a content preparation module for pre-encrypting the content offline to form pre-encrypted content (see for example; col 6 ln 57-65 and col 8 ln 7-42);

an on-demand module receiving the pre-encrypted content from the content preparation module (see for example; remote server fig 4 and col 6 ln 57-65), for storing, and transmitting the pre-encrypted content to the subscriber terminal when authorized (see for example; col 7 ln 20-34);

and a conditional access system for providing a periodical key to the encryption renewal system (see for example; col 4 ln 44-59 and col 8 ln 47-58).

Colligan further discloses an encryption renewal system to generate control messages allowing the pre-encrypted content to be decryptable for a designated duration (see for example; col 8 ln 41-56 and col 9 ln 11-16). Colligan does not explicitly teach an encryption renewal system generating time limited entitlement control messages (ECMs) allowing the pre-encrypted content to be decryptable for a time limited designated duration. Colligan discloses a means of decrypting by providing information on creating the decryption key (see for example; col 7 ln 27-34) and that there is a need to provide access restriction due to billing for premium channels (see for example; col 4 ln 44-59).

However, Wasilewski teaches a system for generating time limited entitlement control messages for decrypting an encrypted content for a time limited designated duration (i.e., control words in an ECM) [column 4, lines 26-39 and column 6, lines 33-56]. Wasilewski further teaches generating time ECMs in synchronization with providing periodical key (for example Multi-Session key (MSK)) [column 6, lines 33-56, column 9, lines 10-22 and column 15, lines 20-30]. Therefore It would have been obvious to one having ordinary skill in the art at the time the invention was made to employ the method of generating time limited entitlement control messages (ECM) in synchronization with providing periodical key (MSK) as taught by Wasilewski within the system of Colligna in order to allow decryption of content for a certain period of time and further provide time limited ECMs to be used for a limited time period decryption of content.

8. As per claims 2 and 42, Colligan further discloses system wherein communication network is a cable network for distributing audio/video content from a cable central office to all or a subset of subscriber terminals (see for example; fig 4 and col 3 ln 50-65).

9. Claims 3, 5-14 and 17-19, are rejected under 35 U.S.C. 103(a) as being unpatentable over Bertram US PUB 2003/0140340 A1 in view of Wasilewski et al. US Patent 6,516,412 B2 (hereinafter Wasilewski).

10. As per claim 3, Bertram discloses a method of delivering content from one or more cable systems to subscriber terminals within the cable systems (see for example; abstract and fig 1), the cable systems being communicatively coupled to an offline encryption device (see for example; 130 fig 1), the method comprising;

receiving by a first cable system, a request for the content from a first subscriber terminal of the first cable system (see for example; 407 fig 4 and paragraphs 51-52),

pre-encrypting, by the offline encryption device, the content to form pre-encrypted content prior to the step of receiving a request (see for example; paragraph 63); generating an encryption record containing parameters employed for encrypting the content; based on the encryption record and a first key information (see for example; encryption algorithm, paragraphs 45-46; an encryption record must be generated in order to carry out encryption and carry out synchronization with the generation of descrambling messages) generating one or more control messages for permitting access to the pre-encrypted content (see for example; paragraphs 46-47); and transmitting the pre-encrypted content associated with the one or more control messages to the first subscriber terminal for decryption of the pre-encrypted content (see for example; paragraphs 31 and 47). Bertram does not explicitly teach generating time limited control messages for permitting access to the pre-encrypted content. However, Wasilewski teaches a system for generating time limited entitlement control messages for decrypting an encrypted content for a time limited designated duration (i.e., control words in an ECM) [column 4, lines 26-39 and column 6, lines 33-56]. Wasilewski further teaches generating time limited ECMs in synchronization with providing periodical key (for example Multi-Session key (MSK) [column 6, lines 33-56, column 9, lines 10-22 and column 15, lines 20-30]. Therefore It would have been obvious to one having ordinary skill in the art at the time the invention was made to employ the method of generating time limited entitlement control messages (ECM) in synchronization with providing periodical key (MSK) as taught by Wasilewski within the system of Bertram in order to allow decryption of content for a certain period of time and further provide time limited ECMs to be used for a limited time period decryption of content.

11. As per claim 17, Bertram discloses pre-encrypting, by the offline encryption device, the content to form pre-encrypted content prior to the step of receiving a request (see for example; paragraph 63);

generating an encryption record containing parameters employed for encrypting the content; based on the encryption record and a first key information (see for example; encryption algorithm, paragraphs 45-46; an encryption record must be generated in order to carry out encryption and carry out synchronization with the generation of "descrambling" messages) generating one or more entitlement messages for permitting access that allow decryption of the content (see for example; paragraphs 46-47);

a conditional access system that allows for providing information included in the entitlement messages by the means for generating (see for example; paragraph 47) and transmitting the pre-encrypted content associated with the one or more control messages to the first subscriber terminal for decryption of the pre-encrypted content (see for example; paragraphs 31 and 47) and means for receiving the pre-encrypted content from the means for pre-encrypting (see for example; fig 1 and paragraph 29), forwarding the records to the means for generating which generates the first and second entitlement messages for forwarding to the subscriber terminal (see for example; paragraph 62-63 the encryption record must be forwarded in order to generate corresponding entitlement messages used by the conditional access system).

As for a first and second content, Bertram discloses encryption of different content (see for example; paragraph 60). However, Bertram is silent on the means of encrypting the second content. The means of encrypting further content by the same means would have been obvious to one of ordinary skill in the art at the time of the applicant's invention because it would have allowed for encryption of different content without changing system architecture. Therefore, one of ordinary skill in the art at the time of the applicant's invention would have realized the duplication in generating a second pre-encrypted content. Bertram does not explicitly teach generating time limited entitlement messages for permitting access to the pre-encrypted content. However, Wasilewski teaches a system for generating time limited entitlement control messages for decrypting an encrypted content for a time limited designated duration (i.e., control words in an ECM) [column 4, lines 26-39 and column 6, lines 33-56]. Wasilewski further teaches generating time limited ECMs in synchronization with providing periodical key (for example Multi-Session key (MSK) [column 6, lines 33-56, column 9, lines 10-22 and column 15, lines 20-30]. Therefore It would have been obvious to one having ordinary skill in the art at the time the invention was made to employ the method of generating time limited entitlement control messages (ECM) in synchronization with providing periodical key (MSK) as taught by Wasilewski within the system of Bertram in order to allow decryption of content for a certain period of time and further provide time limited ECMs to be used for a limited time period decryption of content.

12. As per claim 5, Bertram further discloses wherein the first key information is provided by a conditional access system (see for example; paragraph 47) that uses the key information to control the first subscriber terminal (see for example; paragraph 47; the set top terminal

descrambles the content thereby prohibiting unauthorized users from viewing the encrypted content).

13. As per claim 6, Bertram further discloses wherein the key information is for a key that is periodical and valid for a designated duration (see for example; paragraph 63).

14. As per claim 7, Bertram further discloses wherein the designated duration is shortly before, contemporaneous with, or shortly after the first key is changed by the conditional access system (see for example; paragraph 63).

15 As per claims 8, 9 and 11-13, Wasilewski further discloses time limited ECMs for conveying information to a first subscriber terminal to compute a key, and further discloses changing the key information after a designated duration and retrofitting a second time limited ECM to the encrypted content and synchronizing time limited ECMs with changing of key information [column 4, lines 26-39 and column 6, lines 33-56].

16. As per claim 14, Bertram further discloses wherein the step of generating an encryption record is by an offline encryption system (see for example; paragraphs 46 and 63).

17. As per claim 18, Bertram does not explicitly teach generating a third entitlement message. However, Bertram discloses pre-encryption of multiple content (see for example; paragraph 60). Therefore, one of ordinary skill in the art at the time of the applicant's invention would have realized such generating for a third content.

18. As per claims 19, Bertram further discloses an expiration of the first entitlement messages (see for example, paragraph 63).

19. Claims 4 and 15-16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bertram, US Publication 200310140340, in view of Wasilewski US Patent 6,516,412 B2 as applied above and further in view of Dunn et al (hereinafter Dunn), US Patent 6,154,772.

20. As per claim 4, Bertram and Wasilewski disclose a means of distributing content using a cable system as described above (see claim 3). Bertram is silent on the details of a second cable system. However, communication of content to multiple cable systems is well known in the art. Dunn et al discloses delivering content to multiple cable systems (see for example; fig 2 and col 2 ln 45-60) to reduce bandwidth and further gain control of distribution of cable and/or satellite content to subscribers (see for example; col 2 ln 7-31). Bertram discloses such a system communicating within a network (see for example; fig 5 and paragraphs 29-30). Communication between multiple networks is well known in the art. One of ordinary skill in the art at the time of the applicant's invention would have been able to perform pre-encryption using the system of Bertram and Wasilewski for a second cable system of Dunn. It would have been obvious to one of ordinary skill in the art to employ the second cable system of Dunn within the system of Bertram and Wasilewski because it would have provided a means of freeing bandwidth when broadcasting to multiple subscribers by offsetting transmission between different cable systems.

21. As per claims 15 and 16, Bertram-Wasilewski-Dunn teach the method as described above. Furthermore, Bertram discloses limiting access to the pre-encrypted content (see for example: paragraph 47).

22. Claims 33 and 34 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bertram, US Publication 200310140340, in view of Wasilewski US Patent 6,516,412 B2 as applied above and further in view of Colligna US Patent 6,415,031 B1.

23. As per claim 33, Bertram and Wasilewski disclose the claimed limitations as described above (see claim 3). Bertram does not explicitly teach pre-encrypting being carried out using a third key, and the encryption record containing information about the third key. Colligan further discloses encryption using multiple keys, wherein an encryption record contains information about the keys (see for example; 8 ln 23-41). By using different keys many attacks are inhibited since once a key is obtained through an attack, the key is no longer valid. It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the multiple key encryption of Colligan within the system of Bertram and Wasilewski because it would have increased security by inhibiting attacks through changing keys.

24. As per claim 34, Bertram-Wasilewski-Colligan discloses the claimed limitations as described above (see claim 33). Colligan further discloses translating the third key into the first key information (see for example; col 8 ln 23-41). One of ordinary skill in the art at the time of the applicant's invention would have realized such translating must be present for providing descrambling messages of Bertram.

## *Response to Arguments*

25. Applicant's arguments filed January 04, 2006 have been fully considered but they are not persuasive.

26. With respect to claims 1, 2, 41 and 42, applicant argues that the art on record fails to teach an encryption renewal system performing periodic entitlement control message renewal in synchronization with a conditional access system and without re-encrypting the pre-encrypted content. Examiner disagrees.

The examiner cites MPEP 2173.05(i) :

*"Any negative limitation or exclusionary proviso must have basis in the original disclosure. If alternative elements are positively recited in the specification, they may be explicitly excluded in the claims. See In re Johnson, 558 F.2d 1008, 1019, 194 USPQ 187, 196 (CCPA 1977) ("[the] specification, having described the whole, necessarily described the part remaining."). See also Ex parte Grasselli, 231 USPQ 393 (Bd. App. 1983), aff'dmem., 738 F.2d 453 (Fed. Cir. 1984). The mere absence of a positive recitation is not basis for an exclusion. Any claim containing a negative limitation which does not have basis in the original disclosure should be rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement."*

The amended phrase clearly recites a negative limitation. Indeed, the specification must contain a full, clear and concise description of the claimed subject matter. The specification does not literally or implicitly describe an encryption renewal system performing periodic entitlement control message renewal in synchronization with a conditional access system and **without re-encrypting the pre-encrypted content.**

27. With respect to claim 3 and 17, Applicant argues that the art on record fails to teach generating one or more time limited control messages for permitting access to the content or periodically retrofitting a second time limited entitlement control message to the pre-encrypted content for permitting access to the pre-encrypted content after the first key information expires, and performing periodic entitlement control message renewal. Examiner disagrees.

28. Examiner would point out that Bertram teaches pre-encrypting, by the offline encryption device, the content to form pre-encrypted content prior to the step of receiving a request (see for example; paragraph 63). Furthermore, Wasilewski teaches a system for generating time limited entitlement control messages for decrypting an encrypted content for a time limited designated duration (i.e., control words in an ECM) [column 4, lines 26-39 and column 6, lines 33-56]. Wasilewski further teaches generating time limited ECMs in synchronization with providing periodical key (for example Multi-Session key (MSK) [column 6, lines 33-56, column 9, lines 10-22 and column 15, lines 20-30]. In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986). Examiner asserts that the art on record teaches the claim limitations and therefor the rejection is respectfully maintained.

## *Conclusion*

**THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO

MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Beemnet W. Dada whose telephone number is (571) 272-3847. The examiner can normally be reached on Monday - Friday (9:00 am - 5:30 pm).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Beemnet Dada
April 1, 2006

HOSUK SONG
PRIMARY EXAMINER